Each employee is responsible for promptly reporting an incident affecting the Department of Treasury, its resources and property. An incident, for purposes of this Policy, is any adverse event whereby some aspect of physical or financial security is threatened; confidentiality or privacy of data is violated; data is manipulated or lost; financial resources or items of value are lost, misused or stolen; or unauthorized or unlawful activity. Michigan Civil Service Commission Rule 2-10 provides for protection from reprisal and/or disciplinary action against state classified employees reporting an incident involving public funds or property. The Whistleblower's Protection Act, Public Act 469 of 1980, as amended, provides the same protection for unclassified employees.

Goals of incident reporting include:

- Facilitating appropriate reporting of incidents
- Confirming or dispelling whether an incident has occurred
- Coordinating response to certain incidents
- Protecting confidentiality and privacy
- Minimizing disruptions to normal business operations
- Providing accurate reporting and useful recommendations
- Mitigating risks through corrective actions
- Deterring future incidents.

Incidents include but are not limited to threats; missing, lost or misplaced negotiable instruments; missing or unauthorized disclosure of confidential or sensitive information; unauthorized probing and browsing; theft; unlocked secure areas; altered or destroyed input, processing, storage or output of information; changes to information system software without the knowledge of or approval by the Treasury Business Owner; knowingly causing or spreading a computer virus; or attempted or unauthorized entry into or an information attack on an information system. They affect the following areas:

- Safety
- Financial resources
- Public trust
- Stakeholder confidence
- Legal liability
- Personal liability.

When an employee discovers or becomes knowledgeable of an incident, he or she must immediately notify his or her supervisor. However, if it is suspected that the incident involves the immediate supervisor, contact the next management staff member in the chain. Immediately contact the Department of Information Technology (DIT) Helpdesk for suspected or actual computer-related incidents such as viruses, worms, Trojan horses and other malicious software/source code, then notify the Office of Security. DIT staff are responsible for defining appropriate procedures for addressing computer information attacks or denial of service attacks; identifying physical and electronic evidence to be gathered; monitoring, repairing and mitigating any damage from an information attack; and/or minimizing or eliminating the information technology vulnerability, where possible.

If an incident affects other agencies, management staff must notify affected entities so they can take appropriate action. When apprising others of the existence of an incident, make every attempt to provide clear and concise information to assist in dissemination of this information within their respective organizations.

If an incident occurs, either suspected or actual, that constitutes an immediate threat to critical resources, materials or data, follow proper emergency procedures. Management must immediately notify the Bureau Director or Deputy Treasurer through the appropriate chain of command and immediately begin investigation of the reported incident.

Incident Reporting

The Office of Security must communicate information and alerts related to an incident having potential widespread implications to all Department staff. Prepare Parts 1 and 2 of form 4000 INCIDENT REPORT and submit it to the Office of Security for purposes of immediate notification of an incident.

After incident resolution, the Division Administrator or Office Director must prepare and submit a final form 4000 to the Office of Security. The report should provide:

- When the incident occurred or was discovered
- Who was involved
- Location of the incident
- Description of the incident
- Action taken
- Incident impact (i.e., likely consequences, affect on other agencies or organizations, etc.)
- Post-incident recommendations to lessen the likelihood of a similar incident.

Report human resources incidents to the Human Resources Division instead of the Office of Security and the Office of Internal Audit, Department of Management and Budget (DMB). (Refer to Bulletin BT-03049 in the Employee Handbook and Procedure PT-03095 in the Employee or Supervisor Handbook for additional guidance.)

Management must follow up with pertinent staff, including staff who reported the incident, and inform them of the facts involving the incident and its resolution.

To improve incident response, management should document and incorporate lessons learned in divisional or office guidelines.

Incident Information Distribution

Always direct legislative, press or broadcast media inquiries to the Public Information Officer (Press Secretary) for the Department. The Public Information Officer acts as a single point of contact and response for the Department.

The Office of Security must issue quarterly reports on incidents occurring within or affecting the Department. Periodically, the Office of Internal Audit, DMB, must review incident reports to determine whether issues exist that merit further investigation and remediation.

End